

Informations utiles sur l'usage de votre machine

### **Introduction**

Ce guide est destiné à sensibiliser tous les administrateurs au niveau de certains sujets concernant votre dédié et son administration. Au vu du grand nombre de demandes traitées quotidiennement, le support désire vous aider afin d'éviter certaines erreurs souvent commises et qui peuvent entraîner des conséquences graves pour votre machine et entraîner une inaccessibilité inutile. Il est également destiné à vous rappeler quelques gestes administratifs basiques mais vitaux.

### **Mots de passe**

Conservez bien votre mail d'installation. N'oubliez pas qu'il y a plusieurs mots de passe et que celui de Webmin et celui de SSH ne sont pas forcément identiques. Si vous personnalisez vos mots de passe vous devrez les conserver et mémoriser. Pourquoi ? Car il nous est impossible de récupérer vos mots de passe personnalisés et qu'il faut forcément intervenir sur la machine afin de les restaurer, ce qui entraîne des frais.

### **Nic-handle**

Il est aussi très important de ne pas indiquer dans votre NIC-handle une adresse email contenant les domaines qui sont hébergés sur la machine. Pourquoi ? Si la machine est inaccessible ou si votre domaine est injoignable pour une quelconque raison, nous ne pouvons pas vous contacter, ayant comme seul contact l'adresse mail de votre NIC-handle.

### **Le backup**

La chose la plus importante sur votre machine sont vos données. Il est impératif d'avoir un backup de ces données afin de pouvoir restaurer en un temps minimal tous les services sur votre machine. Imaginez par exemple que vous fassiez une mauvaise manipulation et perdiez un dossier entier contenant votre site le plus important ! Votre backup vous permettra de restaurer au plus vite le dossier perdu. Il y a plusieurs possibilités de faire un backup. Nous vous proposons par exemple :

- le backup hebdomadaire,
- l'installation d'un disque de backup,
- l'utilisation d'un système RAID.

### **La manipulation des données et fichiers**

Avant de faire une modification dans un fichier, vous devriez toujours penser à ce qui peut arriver si les modifications ne sont pas correctes. Votre serveur web par exemple peut être inaccessible suite à des mauvais paramètres dans le fichier de configuration. Nous vous conseillons de faire une copie du fichier que vous avez prévu d'éditer. Avec cette petite astuce il vous sera possible de restaurer très rapidement la configuration précédente.

### **Mise à jour du système**

Très important aussi, mettez régulièrement votre release ainsi que votre kernel à jour afin de ne pas donner l'occasion à un hacker de s'introduire et aussi pour fixer des bugs au niveau du système. Vous pouvez soit vous servir de ces guides : ReleasePatchSecurite et KernelMethodes soit nous confier la sécurité de votre machine en optant pour l'offre Sécurité Totale.

### **Sécurité site**

Accordez également une grande importance à la sécurité au niveau des scripts, portails et failles dans les langues de programmation que vous utilisez pour vos sites. SecuriteSite est un guide qui traite de ce sujet. Grâce à notre système de monitoring RTM vous pouvez désormais découvrir des backdoors. Les informations récupérées par RTM sont disponibles dans votre Manager, section serveur dédié. Bien sûr vous disposez aussi

de guides dans la section serveur dédié, sous-catégorie Sécurité et la possibilité de nous confier la résolution de votre problème via le service InfogéranceS.

### **Compilation et installation de softs**

Avant l'installation ou une recompilation d'un software sur votre machine, vérifiez les conséquences que cela peut entraîner. Prenez les mesures adéquates. Si vous êtes néophyte et que vous avez absolument besoin d'une installation ou autre vous pouvez confier l'intervention à notre service d'infogérance.

### **Contact support**

Quand vous contactez le support indiquez le plus de détails techniques possibles. Indiquez le numéro de la machine et en cas de problème avec un site le nom de domaine ou encore l'adresse mail exacte sur laquelle vous rencontrez des problèmes. N'hésitez pas à expliquer les manipulations que vous avez déjà effectuées ou expliquer en détail ce que vous désirez obtenir comme résultat. Notre support se fera une joie de vous guider et de vous conseiller. N'ouvrez si possible qu'un seul échange à la fois et évitez d'auto-répondre à votre message. Ceci peut éviter des longues attentes et la perte d'informations ou la double prise en charge.

### **Mode Rescue et RTM**

Nous avons élaboré des systèmes qui sont destinés à la réduction des inaccessibilités de votre machine lors d'une panne et pour reprendre à tout moment la main sur votre machine. Vous avez donc à votre disposition le RTM qui nous permet de détecter rapidement des problèmes au niveau de votre hardware et le ModeRescue qui vous permet de restaurer votre système à tout moment.

### **Mise en garde**

- commande dangereuse

Attention à ne jamais utiliser la commande `rm -rf /*`. Cette commande provoque la destruction récursive de tous les dossiers, sous-dossiers et fichiers à partir de la racine / et avec l'option `-rf` la commande sera appliquée sans vérification quelconque. Elle entraîne donc la destruction complète de toutes vos données.

- changer le repertoire personnel du root

Il arrive que les administrateurs changent le répertoire de connexion root qui est d'origine /root. Ceci empêche ensuite la connexion avec la clef ssh (InstallClefOVH) que nous utilisons pour intervenir sur votre machine en cas de besoin. De même si vous empêchez la connexion ssh pour le root ou si vous modifiez le port de connexion pour SSH qui par défaut est le port 22.

### **Conclusion**

En respectant ces quelques gestes d'administration basiques vous pouvez éviter des problèmes avec votre machine. Suivez les conseils de tous nos guides. Ceux-ci sont réalisés pour vous permettre d'obtenir les meilleurs résultats au niveau des performances de votre machine.